解　説

金融決済システムとセキュリティ対策の現状

岡崎悦夫

The Financial Payment and Settlement System in Japan and its Measure against Security

Etsuo OKAZAKI

ABSTRACT

The financial payment and settlement system is one of the important social infrastructures supporting economic activity. When it does not function smoothly, large problems arise concerning economic activity. Moreover, because of the globalization of the economy and finances, the problem is not only domestic. Progress in information communication technology has contributed greatly to the efficiency of the financial payment and settlement system. On the other hand, new types of financial high-tech crime, such as forged money-cards and fraudulent mail schemes, threaten these financial institutions. The system must also be equipped to deal with physical threats, such as natural disasters and large-scale terrorism. Financial institutions are aiming to create safer and more efficient financial settlement systems.

KEYWORDS: financial payment and settlement system, measure against an information security, forged money card, internet banking, BCP

1．『決済』の重要性

日本銀行では，政策・業務運営の参考とするため，国民各層の意見や要望を幅広く聴取するよう努めており，その一環として，年４回，全国の20歳以上の個人4,000人を対象に，生活の状況や意識について世論調査を行っている。最近の生活意識調査で，「日本銀行の業務について知っていますか？」という質問に，「ほとんど知らない」と答えた人は７割程度であった。それぐらい日本銀行が何をやっているのかというのは分かりにくいようである。なお，日本銀行は，「ニッポンギンコウ」が正式の呼び方である。

日本銀行とは，教科書的な説明では３つの機能に区分される。第１に発券銀行である。発券銀行とは，銀行券すなわちお札を発行する銀行である。第２に「銀行の銀行」，そして第３が「政府の銀行」である。本講演の主題である「決済システム」というのは，その「銀行の銀行」というところに非常に拘わるものである。本日の講演をお聞きになった方々には，今後，生活意識調査のアンケートに回答する機会があれば，「日本銀行の業務を多少知っている」という項目にマルをつけて頂きたいと思う。

日本は「自由・資本主義経済」であり，その中で私たちは自由に生活をエンジョイしているが，私たちにとって「満足な生活」をする最大の経済的条件は何か，ということを考えたことがあるであろうか。それは「分業」ということである。「ロビンソンクルーソー物語」は，無人島で一人生活するといった境遇に陥った人の物語であるが，無人島であるから自分ひとりしかいない。一人で生活するということは，欲しいものは自分で作るしかない。技術力がいくらあっても，全てを自分で作るには，時間もかかり，難しいということになる。

2006年10月25日受付，2006年12月５日最終受付
岡崎悦夫　日本銀行徳島事務所
Etsuo OKAZAKI, Nonmember (Tokushima Office, Bank of Japan., Tokushima, 770-0901 Japan).
四国大学経営情報研究所年報　No.12　pp.103-116　2006年12月

今の日本に限らず，世界でどういうことが起きているか，それは「得意な人」つまり各分野の専門家が，社会的な「分業」体制の中で，得意なものを作っている。専門家はその分野で優れている人だから，「無駄のない作り方」をする。それが一番効率的で無駄が少ない。有限の資源を効率的に使って社会全体での生産量を最大にして，それを皆で分ければ，欲しいものが比較的容易に手に入り，より多くの人が満足できるというわけである。当然，分業した成果を「交換」しないといけない。自分の欲しいものを手に入れ，相手が欲しいものを譲るには，交換という行為が不可欠である。交換とは別の言葉でいうと「取引」である。その取引には，必ず決済というものが伴う。モノを売った場合にはお金を受け取る権利が生じ，それを債権という。モノを買った人はお金を支払う義務が生じ，それを債務という。この債権と債務を解消することを「決済」という。

資料１

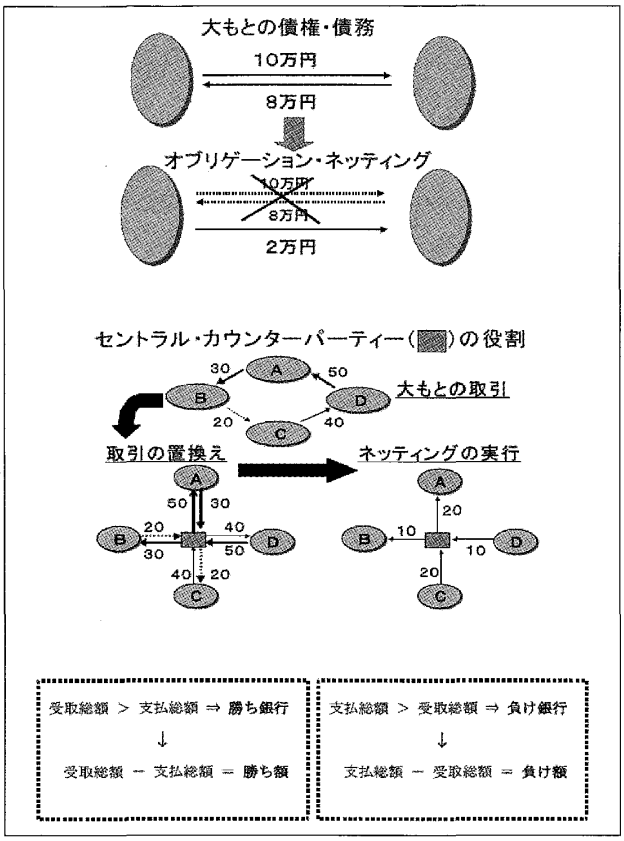
２．決済システムと情報処理

今の社会で決済がうまく行われなくなると，日頃の生活に相当な支障をきたす。欲しいモノが満足に手に入らないという状態になってしまうわけである。

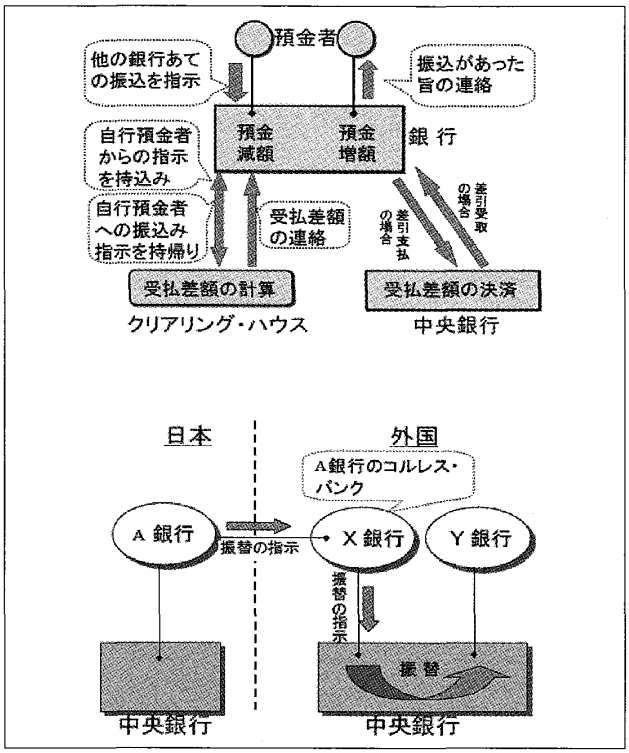
決済は，大方の場合，代金を支払うということであるが，どのように行っているのであろうか。小口のものは現金（キャッシュ）を支払うことで片づくが，多くの場合，銀行の振替機能を使って，自分のお金を預けている銀行や信用金庫の預金残高を減らし，同額を相手の預金口座に付け替え（振替）ることで，決済を行っている。

「相手の口座にお金を振り込む方法」は大きく２通りあって，自分が直接銀行に対して振替指図をする方法，つまり銀行に指示をして相手の口座に入金するという方法と，受け取る人に銀行に対する振替の指図書を渡すやり方がある。それを図にしたのが資料１である。銀行に直接指示するためのアクセス手段としては，銀行の窓口，ATM，コンビニ，携帯電話，インターネットなどがある。間接的な指図とは，クレジットカード等のカード類，手形，小切手等の手段で銀行預金を動かして決済を行うことである。

当然，大多数の人間が振替機能を使って決済しているわけだから，取扱い件数は相当な量となる。それらを一件一件処理するのは，かなり大変な作業である。とくに，Ａさんの取引銀行とＢさんの取引銀行が異なる場合は，銀行間で預金を移し替える必要があり，さらに大変である。そうした本来の決済に伴う負担を軽減するために，資料２のような，「ネッティング」という方法がある。これは，一件一件処理すると大変なので，受・払を差し引くことで取引の件数や金額を小さくしておいて，最後に資金のやり取りを行うという形をとる，オブリゲーション・ネッティングという概念である。この方式は，取引数が多いほど効果的となるが，受・払の全てが同じ決済日であることが必要である。また，相対のケースだけでなく，これを複数の銀行間で行うことが可能である。そ



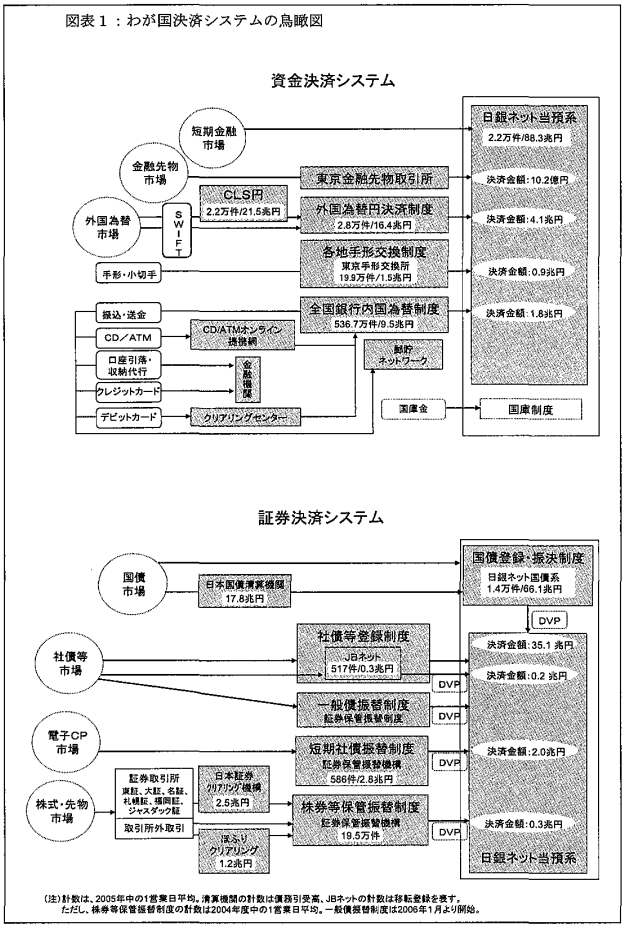
資料２



資料３

の際には，ネッティング結果として新たに作り出される債権・債務の帰属に関する法的な対処として，セントラル・カウンターパーティが導入される。図の真ん中にある四角の部分が中心となって，取引を全部ネットアウトしていき，最後は右側の図のように，少額の決済額となる。受取額の多い銀行が勝ち銀行，支払額が多い銀行が負け銀行である。負け銀行は負け額を支払い，勝ち銀行へは勝ち額が入金されるということである。この銀行間の最終決済をどのようにするかというと，これが，前述した日本銀行の「銀行の銀行」としての役割のひとつであるが，日本銀行が各金融機関から預け入れられている預金（当座預金）の残高を増減させることで決済するということである。資料３の上の図がイメージ図である。受・払指示の差額を，最終的に日本銀行の当座預金で決済するわけである。資料３の下の図が，海外との取引に伴う決済の場合である。このケースでも基本的に同じやり方である。ただし，日本銀行が直接海外の中央銀行と資金のやり取りを行うのではなく，民間ベースで提携した銀行を使って決済を行うという形をとる。いずれにしても，最終的な決済は，中央銀行（日本では日本銀行）の当座預金で行うケースがほとんどである。なお，モノを受け取るのと，お金を支払うのに時間差が生じる場合，決済が行われない危険性が存在することになる。それらをスムーズに処理するために，「金融」が介在する。金融とは文字通り「お金を融通する」ということである。信用のない人はお金を融通して貰えない（借りられない）ので，持っている現金もしくは預金の範囲内でしか，モノを購入できないという制約を受けることになる。つまり，「信用は大切だ」ということである。

ここまで，「決済」をミクロ的に説明してきたが，それをマクロでみると，資料４のようになる。これは，わが国決済システムの鳥瞰図である。上図が資金の決済システムで，下図が証券（国債や社債）の決済システムである。日銀ネット当預系は，日銀の当座預金を動かすシステムのことで，2.2万件／88.3兆円と書いてあるのは，下記（注）のとおり，日銀ネットを利用した短期金融



資料４

市場における取引の2005年中の１日の平均取扱高である。その他の市場等の取引の最終決済分を合わせると，１日当り100兆円を超える金額の決済が日銀ネット上で行われているというわけである。なお，上図左側の外国為替市場では，１日約１兆９千億ドルもの取引がなされており，それらの最終決済も日銀ネットで処理されているということである。

この鳥瞰図の中で，皆さんの身近な取引を処理している仕組みは，全国銀行内国為替制度というもので,利用しているシステムは「全銀システム」と言い，オンラインのネットワークシステムである。このシステムは1973年に作られたのだが，これが皆さんの生活に多大なメリットをもたらしている。全国津々浦々の銀行店舗がカバーされており，そのため日本では，銀行決済・振替が当日実行されるわけである。これは世界でも，そうそう例がない自慢できるシステムである。このシステムで処理された結果の，銀行間の最終決済についても日銀ネットが処理するという仕組みになっている。

資料４の下図は証券決済システムである。証券と言われるものには，国債や社債，株式等色々なものがある。取引においては，証券という形の「モノ」が動くのだが，その裏では必ずお金が動く。そのお金についても，最終的に日銀の当座預金で処理する仕組みになっている。

３．安全で効率的な決済システムを目指して

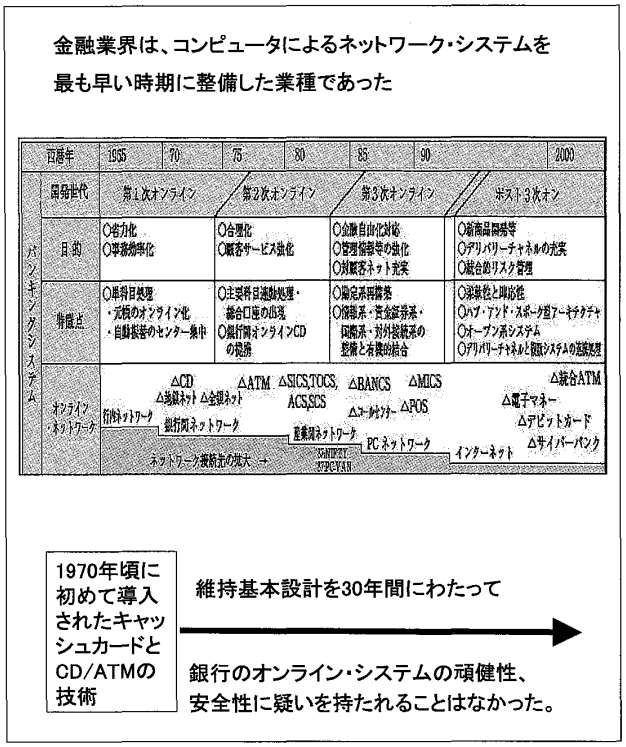
前章では，知らず知らずのうちに恩恵をうけている金融決済システムの概要を述べた。これらのシステムでは，膨大な取引を効率的に処理しているのだが，決済量が増えてくると，一方ではリスクも増える。また，システム技術の進歩に伴うリスクの増加もある。それらのリスクへの対処が金融界に求められている。

金融界は，コンピュータによるネットワークシステムというものを最も早く取り入れた業界で，全銀システムが1973年にスタートした。その後も技術進歩の流れに従って，様々なシステムを作ってきている。しかし，1970年代に導入されたキャッシュカード，ATM等，つまり，「磁気ストライプ」の技術を前提とした基本設計は，それ以降ほとんど変わっていない。要は30年間これが使われてきたというのが，日本の現状である。その間，システムの安全性等に疑いを持たれたことは，最近まではなかった。しかし，先ほど申し上げたように，様々なリスクが存在するので，それらに予防的に対応していかなければならない状況になっている。

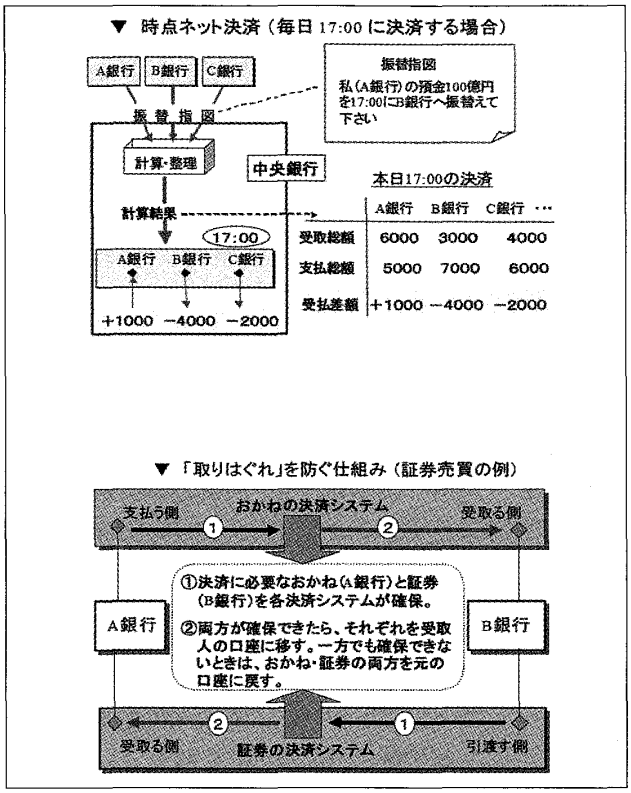
そのリスクを，決済リスク，セキュリティ侵害，BCPの３点に整理して説明する。

３．１　決済リスク

まず，「決済リスク」を説明する。前述の通り，決済は予定通り行われることが前提で，皆さんが平穏に生活を送っているわけであるが，その決済



資料5



資料6

が予定通り行われないことが原因となって，様々な問題が生まれることを，「決済リスク」という言葉で表す。

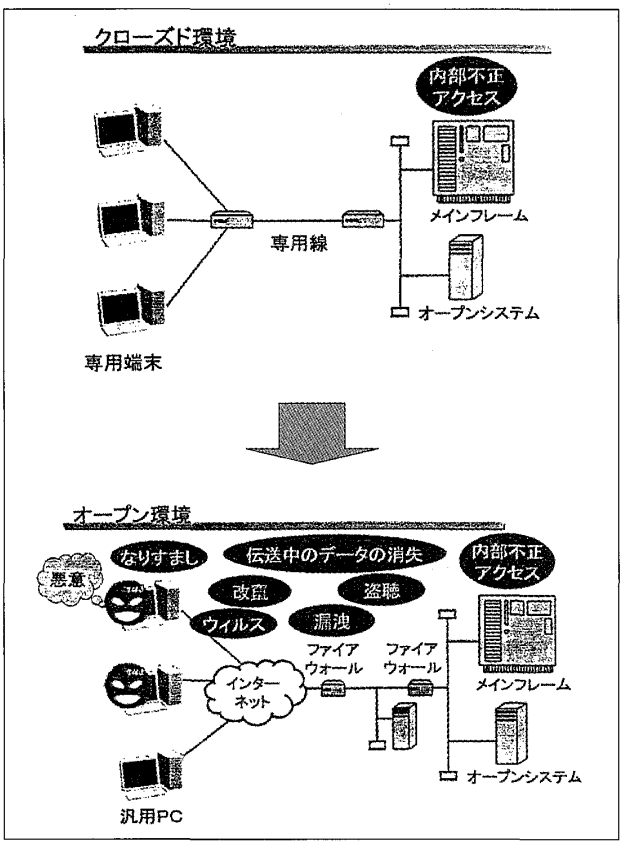
それに似たもので，システミック・リスクというものがある。よく情報システム関連のリスクと間違えられるのだが，システミック・リスクとは，「仕組み上，起きるリスク」である。つまり，ある場所で発生した決済リスク上の問題が，次々と広がっていき，混乱が生じる可能性がある。連鎖のリスクである。ドミノ倒し的に起こる問題の可能性を，システミック・リスクという。

制度的なところから説明すると，資料6の上図は「時点ネット決済」である。これはもう古い仕組みとなったが，かつては，中央銀行の当座預金で決済する際，各銀行から「A銀行にいくら払う」といった振替指図を日本銀行が受けて，一定の時間まで（図では17時）その指図の実行を保留しておく。それらを「ネッティング」して，最終的な受払い額を日銀ネットで一括処理するという仕組みでやっていた。これでは，指図を受けてから決済までに時間差が存在するため，その時間差の間に，ある銀行が倒れて決済ができなくなってしまう事態もあり得る。ひとつでも決済できないとなると，ネッティングの仕組み上，他の決済も成立しないことに繋がっていくことになる。そんな可能性を持っている処理の仕方を続けていたのでは危ないわけであるが，1990年代まで，日本では銀行は潰れないとの神話があり，金融機関の破綻は起こらないということを暗黙の前提としていたのである。しかし，金融不安が現実のものとなり，破綻の可能性を前提にすると，決済までの時間差が存在することは，決済システム全体に悪影響を及ぼすという問題が現実のものとなってきた。それに対処するため，日本銀行では，時点ネット決済を止めて，指図を受けた瞬間に，日本銀行の当座預金をA銀行からB銀行に振り替える仕組みに変えたのである。これは一般に「RTGS」と呼ばれ，「即時グロス決済（Real Time Gross Settlement）」というものである。これが現在の金融決済の向かうべき方向である。

下図は「取りはぐれ」を防ぐ仕組みについてのイメージ図である。これは，証券売買の際，国債や株券の動きに対し，お金が逆方向に動くが，そ

れが同時に行われないと，取引が成立しないというもの。例えば，証券が動いた後でお金を決済しようとした時に相手が倒れると，この決済はできなくなってしまうので，この危険性（リスク）を防ぐ必要がある。つまり，証券とお金を同時に決済する，これを，「Delivery Versus Payment」といい，証券（デリバリー）とお金（ペイメント）を付き合わせるという意味で，略して「DVP」という。目下，この決済方式を取り入れていく取り組みがなされている。これはまだ全ての取引で完成している状況ではない。当然，証券とお金の決済が同時に行われるためには，ペーパーレス化が必要である。証券が物理的に動くには時間がかかってしまうので，電子化された形で動かすというのが，同時決済においての必要条件である。株券を無くして，完全にペーパーレス化を図る取り組みは，2009年頃を目処に作業が進んでいる。なお，国債や社債等一般債は，すでに完全ペーパーレス化されており，同時決済が行われている。

このように，仕組み的に時間差を伴うゆえのリスクを減らそうという動きを，現在続けている。以上が制度面についてである。



資料７

３．２　セキュリティ侵害

もうひとつは，システム技術面でのリスクである。資料７にあるように，1970年代から，金融界はオンラインシステムを着々と導入し，事務効率を引き上げてきた。しかし，これは人手でやっているところを機械に任せるという発想の枠を超えなかったのである。どういうことかというと，当時のシステムは，クローズド環境で構築されていた。要するに，対外的なものとのリンクを取らないといった構成をとり，不正なアクセスを物理的に防ぐ形でシステム化されたのである。この時に，万一の場合の対応を考えなければいけないとすると，それは，システムが倒れた場合のバックアップ問題しかなかったのである。ところが，最近はオープンな環境，端的に言うとインターネットの介在で，それを経由した構成でシステムを使うといった姿が徐々に増えている。金融界は，ファイアーウォール等を設けながら慎重に対応しているわけだが，オープンな環境であるということは，これまで物理的に隔離していたシステム構成のため怖くなかったものが，全てリスクとして認識する必要が高まったということである。改ざんのリスク，ウイルス，漏洩，盗聴などといったものがネットワーク技術においてリスクとなる可能性が出てきたということで，それらへの対応が必要となってきているわけである。

そんな中で，最近の話題としてよく出るのが，偽造キャッシュカード問題である。これは，2003年頃から増加してきた，偽造キャッシュカードによる不正の預金引出という犯罪にどのように対処すべきかという問題である。資料８の左上の表が被害状況である。アンケート結果ではあるが，これによると，17年度通計で552件，被害額６億9000万円である。あえて申し上げれば，被害として少な目の印象があるが，それでも社会問題化した。どういうことかというと，これより少し以前に，プリペイドカード（高速道路・パチンコ店等）が

偽造キャッシュカードによる被害状況

（単位：件、百万円）

	件数	金額
13 年度	1	10
14 年度	4	16
15 年度	111	303
16 年度	437	981
4 ～6 月	56	186
7 ～9 月	74	276
10～12 月	316	390
1～3 月	89	129
17 年度	553	699
4～6 月	108	135
7～9 月	126	160
10～12 月	164	249
1～3 月	154	146

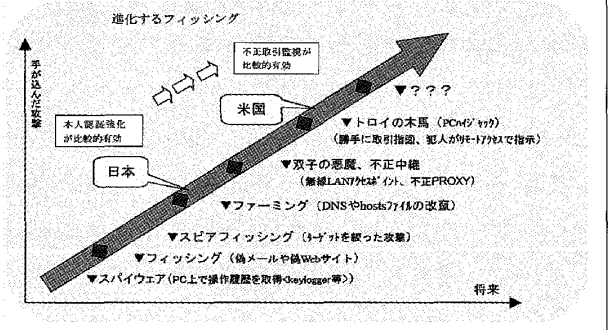
出所：全銀協「偽造キャッシュカードによる預金等不正引出し」に関するアンケート結果

インターネットバンキングの被害状況

（単位：件、百万円）

時期	17 年 4 ～6 月	7 ～9 月	10～12 月	18 年 1～3 月
件数	2	13	16	6
金額	1	12	13	4

出所：全銀協「インターネットバンキングによる預金等不正引出し」に関するアンケート結果



資料 8

偽造されて，ものすごい被害が出た時期があった。数百億円単位の被害が出たという事件なのだが，その時は，別にそれが社会問題化したわけではないのである。というのは，偽造プリペイドカードの被害を蒙ったのが，システムの運営主体，つまりパチンコ店等の業者であったということである。だから国民(消費者)は誰もあえて声をあげなかった。ところが，偽造キャッシュカードを使って預金を引き出された場合には，預金をしている一般国民が直接被害を受けることになるわけで，全ての預金者個人が被害者となり得る問題ということである。つまり，社会全体でみて被害の規模がとくに大きくなくても，被害を受けた個人にとっては大変な被害なのである。これが，言ってみれば社会的に弱い立場である「預金者」を襲ったということで，問題が大きくなったのである。この問題発生に対して，金融機関側の対応も残念ながら後手に回ってしまった。その結果，「預金者保護法」というものが成立した。この法律の正式名称は，「偽造カード等及び盗難カード等を用いて行われる不正な機械式預貯金払い戻し等からの預貯金者の保護等に関する法律」である。相当な落ち度がない限り預金者は守られて，金融機関が補償することになったのである。こうした事態に対して，金融機関はATMから引き出す預金の金額を，一定の金額に絞り込むという対応を採った。つまり，引き出し上限額の引き下げということである。過去には，数百万単位でお金の引き出しができた金融機関もあったようだが，上限額を各金融機関で設定し，万一の場合の被害額を少なくしようという対応である。ただ，これはシステム技術的な防止策ではないので，犯罪そのものは起きてしまうということである。犯罪をどうやって防ぐかということは，本来，セキュリティ対策，つまり技術的な対策をとらなくてはいけないということである。対策の有効性は，手口・手段がどういうものかということにかかる。資料9には，偽造・盗難キャッシュカードの犯罪手口のおおまかな例示をしている。手口の主な分類として，第1は盗用，つまり盗まれるということである。次はスキミング。それから，ATMコーナーに隠しカメラを設置して暗証番号を盗撮するといった手段。さらに，ちょっと質的には違うが，ATMと金融機関本体との通信を盗聴することで，偽造のための情報を手に入れる等，色々な手口がある。

これらに対する有効な対策として，ICカード化が挙げられる。ICカード化が有効であることは間違いないが，今の日本においては磐石とは言えない。なぜかというと，ICカード化していても磁気ストライプ方式併用のケースが多いのが現状だからである。日本では業務提携が進んでおり，色々なシステムと関わっているため，ICカード化した場合，提携先の持っているATMがそれを読み込めるかどうか，読み込めなければ，磁気ストライプを付けておかないと利便性が低くなる。つまり，預金者の利便性を前面に出すと，磁気ストライプの併用を，どうしても断念できないという状況がある。それがひとつの理由。もうひとつは，現実に日本国で発行されているカードの枚数というのは，ざっと見ても3億枚といわれているが，もっと多いかもしれない。それを短期間にICカードに切り替えるということは，到底不可能な

偽造・盗難キャッシュカード犯罪の主な犯行手口とその対策

主な犯行手口		具体的な事例	当面有効なセキュリティ対策			
キャッシュカードの入手	暗証番号の入手		金融機関側		預金者側	
			キャッシュカード	暗証番号	キャッシュカード	暗証番号
カードを盗用	生年月日等の個人情報から推定／ATMでの暗証番号入力を覗き見	過去に実害が生じた事例多数	—	生体認証、ATMでの覗き見防止対策	カードの盗難対策	暗証番号の適正化／ATMでの覗き見への警戒
スキミングによる偽造	生年月日等の個人情報から推定／ATMでの暗証番号入力を覗き見	過去に実害が生じた事例多数	ICカード化	生体認証、ATMでの覗き見防止対策	スキミングの予防	暗証番号の適正化／ATMでの覗き見への警戒
スキミングによる偽造	貴重品ロッカーの暗証番号から推定	2004年から2005年にかけて、あるゴルフ場で継続的に大量のスキミングが行われた	ICカード化	生体認証	スキミングの予防	キャッシュカード用暗証番号を他の用途に利用しない
別途入手した預金口座番号等から偽造	生年月日等の個人情報から推定／ATMでの暗証番号入力を覗き見	1998年、ある企業から漏洩した個人情報を元にカードが偽造され、使用された	ICカード化、磁気カードへの秘密コード付与	生体認証、ATMでの覗き見防止対策	預金口座番号の秘匿	暗証番号の適正化／ATMでの覗き見への警戒
ATMに仕掛けた隠しカメラの映像から偽造	ATMに仕掛けた隠しカメラの映像から入手	2005年から2006年にかけて、首都圏の複数の金融機関のATMコーナーでの盗撮が発覚	隠しカメラの排除、ICカード化、磁気カードへの秘密コード付与	生体認証、隠しカメラの排除	—	—
盗聴した金融機関のATMとの通信内容から偽造	盗聴した金融機関のATMとの通信内容から入手	1982年に、北海道において金融機関が利用する専用回線を盗聴して情報を入手し、カードを偽造・行使	ICカード化、通信暗号化	生体認証、通信暗号化	—	—

資料9

偽造キャッシュカード問題の原因

現在のキャッシュカードによる預金引出しが脆弱であることは、かねて指摘されてきた。

偽造の容易な磁気ストライプカード

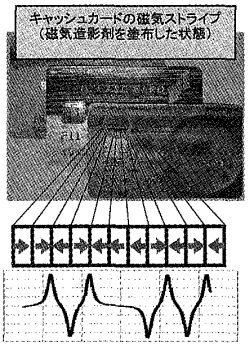
4桁の暗証番号の限界

⇒ 利用者による不適切な設定・運用を排除できないため、推定されたり、金融機関のシステムの外部で漏洩してしまうリスクがある。

銀行のキャッシュカードの暗証番号を何にしているのかの調査

分野	人数	内訳		分野	内訳	
誕生日	89人（46%）	亡夫のない誕生日	53人	その他	2001	映画のタイトル（194人も）
		誕生日をアレンジ	14人		1969	身長166.8cmだから
		家族の誕生日	10人		4789	名前画数、4画7画8画9画
		他人の誕生日	12人		1425	カードを作った時刻 14時25分
電話番号	34人（18%）	自宅	17人		3612	番地、3丁目6番12号
		実家	11人		1789	フランス革命
		彼、彼女	3人		1467	人の世むなし花にの乱
		その他	3人		1134	文化放送
受験番号	7人（4%）	大学受験と模試の受験			0101	丸寺
出席番号	5人（3%）	3419	3年4組19番		0490	民法490条（受取証書の持参人への弁済）
語呂合わせ	13人（7%）	4126	（4人）ヨイフロ		7777	気分で
		1168	ピピンパ			
		2180	ニイハオ			
		909	ククワク			
		439	与作			
		3594	三国志			
		168	イロハ			
		9602	苦労人 など			

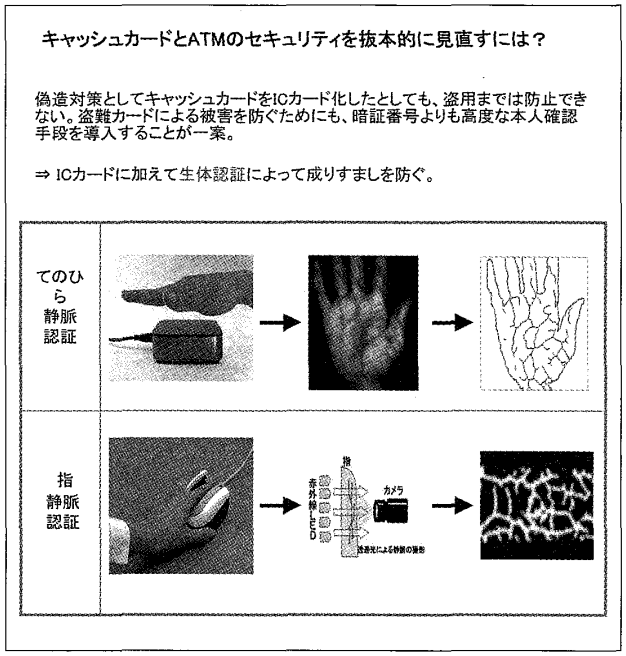
（のべ194人調査） 週刊文春 1995年10月12日号より引用



資料10

話である。ICカード化に踏み切ることが決定している金融機関でも，切り替えに時間がかかってしまう。また，そもそも切り替えに踏み切れるかということも重要な問題なのである。すなわち，コストがかかるということなのである。「どれぐらいの被害が想定されて，金融界が膨大なコストをかけてまで対応しなければいけない事態なのだろうか」という費用対効果を考えてもおかしくはないのである。そうした点を考慮しつつも，金融機関に積極的に対応してもらえるよう，日本銀行は呼びかけているのである。しかし，現実の問題として，3億枚といわれる発行済みカードの中で，IC化されているものは1％強程度，2％にも届いていないのである。また，ICカードに対応したATMの普及も全設置台数の10%程度とまだまだ少ないのが現状である。

次の有効な手段として何があるかというと，生体認証といわれるものである。これは指紋などにより本人確認を行うことを指す。資料11では，私たちの静脈の形状を情報として持ち，それによって本人確認を行えば，カードが盗用されたとしても，本人以外がなりすまして，預金を不正に引き出すということができないという方式を示している。しかし，これにも様々な問題点がある。ひとつは，こういうデータをオンライン情報として取り扱うに当って，提携先システム等との互換性があるかどうか，要は相互運用が可能かどうかという点である。ある銀行は可能でも，提携している金融機関がそこまで対応できなければ成立しない，という問題が出てくる。もうひとつの問題は，これは研究段階の話ではあるが，技術的には，安価な材料で作成された人工指でも，指紋・静脈認証装置が受け入れてしまうケースがあるとの報告がある。したがってこれも完全ではない可能性があるということも分かってきている。さらに，生体認証の導入においても，最大の問題として，膨大なコストがかかるということである。これらを全部クリアしないと，生体認証の導入は難しいということになる。



資料11

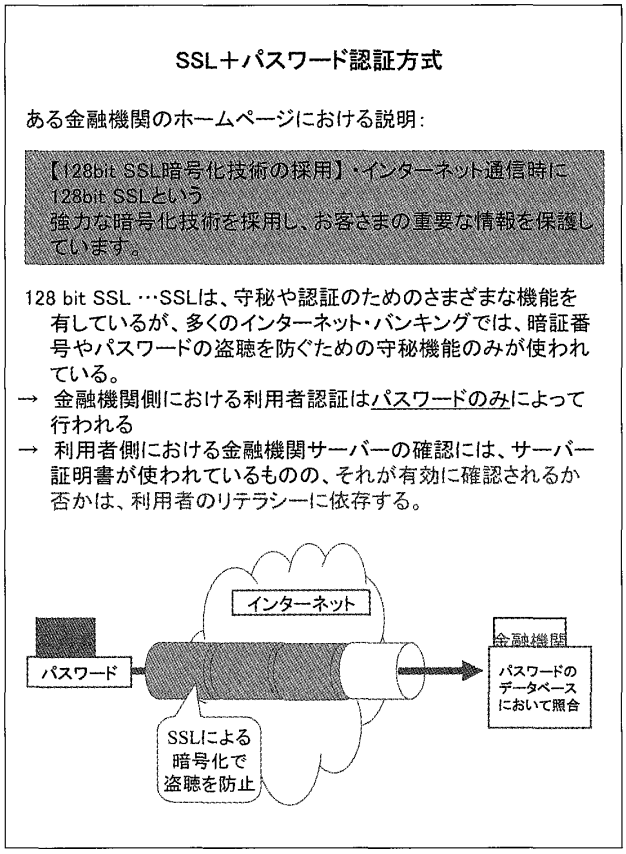
生体認証やICカード化を説明してきたのだが，要は，本人確認というのが一番肝心ということである。本人をどうやって確認するかということ。その方法をシステム技術の話でいうと，二要素認証がポイントである。２つの要素で本人確認をすれば，本人が一応特定できるということである。キャッシュカードと暗証番号というのは，その考え方にある。ただ，あまりにも暗証番号の適正化がなされていないとすれば，それが認証要素たりえないこともあり得るのである。では，認証たり得る要素とは一体何なのか，整理すると３つある。まず，本人が所有しているもの。カードは本人用として発行をしているので，本人が保有しているものとみなすということである。次に，本人の知識。つまり，暗証番号は知識に属するもので，管理がしっかりしていれば，本人が覚えているものでしか利用できないということ。最後は，本人固有の特徴。これが生体認証というものである。これら３つを組み合わせて，多要素認証というケースもあるが，コスト面の問題もあるので，通常使われるのが二要素認証である。要素認証の方式の高度化が進展しつつあるが，業界内の調整に時間を要するものも多いし，投資費用も相当かかるため，一朝一夕には対応できる状況ではない。ちなみに，生体認証を導入している銀行は，全体の２％程度という現状なのである。

次のセキュリティ問題は，インターネット・バンキングに関連した話をしたい。資料８の右上に，インターネット・バンキングにおける犯罪被害状況を示している。件数が，年間40件弱，金額も３千万円程度と，大した被害ではない。ただ，アメリカでは非常に多いようである。インターネット・バンキングにおいて，預金の不正な引き出し事件の発生状況というのは，正確な統計がないのではっきりとは申し上げられないが，ある調査会社が調べた結果では，年間約7,300万人が平均50件以上のフィッシングメールを受け取っているようである。フィッシングメールの手口とは，偽りのメールに騙されて自分に関する情報を発信してしまい，そのために被害にあうということである。被害総額は，年間およそ9,300万ドル，日本円にしてほぼ1,000億円という推計があるようである。アメリカに何でも追随する日本というわけではないが，こういう技術の世界では，同じようなことがいつ起きてもおかしくないのである。先手を打っておかなければならないと思う。資料８の下図は，フィッシングメールといわれる手口の，その技術の進歩というか，手の込んだ攻撃の仕方の変遷を示している。日本では，ファーミングといわれている，接続先情報を改ざんして顧客を不正サイトに誘導する方法，そういう手口が見つかっている段階である。米国では，双子の悪魔とか，トロイの木馬とかが知られている。トロイの木馬という不正プログラムは，PCが感染しても通常は何もしないで潜んでいるが，犯人が外部からリモートでアクセスして不正送金の指図を行ったりすることが可能になるというものである。こういった手口は，プロの犯罪であることが多く，いずれ日本でも被害を受ける可能性があるだろうと思う。というのは，結局，インターネットを介した世界というものは，日本だとか米国だとかは関係ないのである。ボーダレスに世界各国からアクセスできるということなので，その気になれば，

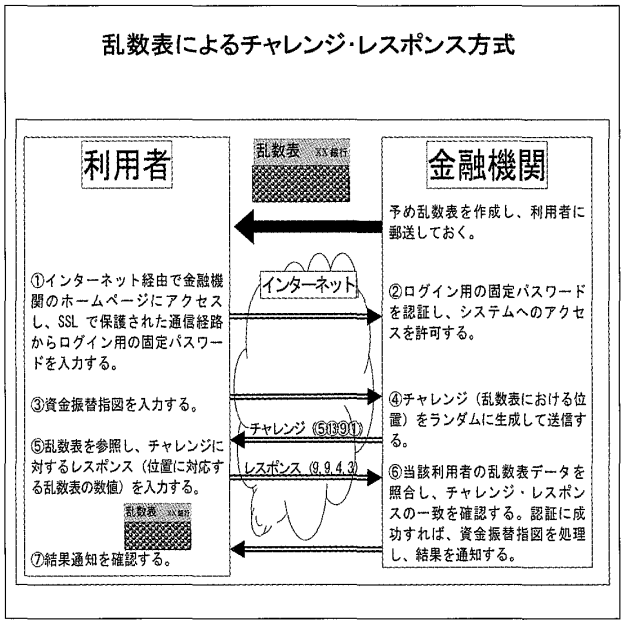
米国から日本のお金持ちを狙うことも可能である。ということで，それに備える必要があるのである。

そこで，どういう対応ができるかというと，資料12である。インターネット・バンキングというものは，1997年頃から出始めて，最初は，厳格な利用者認証方式というものがあり，利用者にとってかなり複雑，繁雑な仕組みであったため，普及しなかったようである。そこで，SSL＋パスワード（SSLとはSecure Socket Layerの略）方式が導入された。インターネット上ではデータを暗号化して，第三者から見られないようにする技術を用い，これにパスワードを付加して認証を行うものである。これにより，2005年3月末現在，256の金融機関が，このインターネット・バンキングサービスを始めていて，1,630万口座あるということであるから，狙う相手はそれなりにいるということになる。この方式では，金融機関における利用者認証がパスワードのみで行われているなど，簡易な使い方で利便性を高めているので，狙われやすい。そのため最近では，もうちょっと手の込んだ認証方式の導入の動きがある。資料13を参考にしていただきたい。これは，乱数表によるチャレンジ方式というやり方である。要は，チャレンジと言われる乱数表の位置をランダムに組成して相手に渡し，その位置情報で特定された数字を入力させることで本人確認をする，という方法を考えているのである。これについても，攻撃者の複数回にわたる取引入力により，いずれは認証データが分かることもありうるという指摘もある。こうしてみると，セキュリティ問題に万全はなさそうだが，いずれにしても，何らかの形で攻撃を受けるということを前提に，金融界としては対応をしなければならないという認識である。

なお，海外ではどういうやり方をしているかというと，ワンタイム・パスワードという方法を認証の標準化としている国（ドイツ）もある。これは，使い捨てのパスワードを組成する機械を相手の企業等に置いて，それを毎回使って，1回毎にパスワードを捨てるというものである。日本でも，一部の大手銀行で採用しようとしているが，普及となると，まだまだ道のりが遠いのが現状である。とりあえず今は被害が小さいので，問題にはなっていないのだが，その危険性を感じなくてはいけないと思っている。



資料12



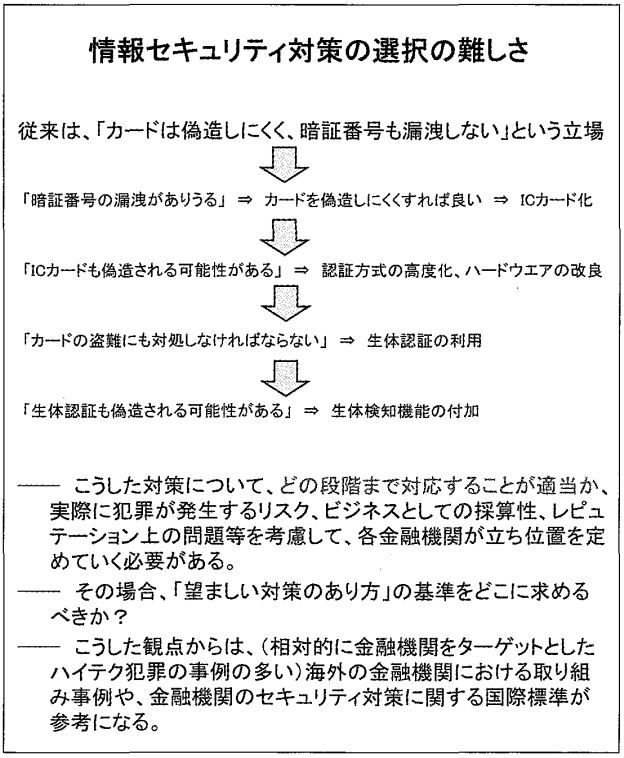
資料13

今までの話をまとめているのが資料14である。言ってみれば情報のセキュリティ対策というのは，いわゆるイタチごっこになっていて，一方で対応費用がかさんできているという現状である。検討のポイントは，ビジネスとしての採算性をどのように考えるかということである。対策のレベル感に関してよく言われているのが，海外の金融機関等で，標準化をして国際的に認知されているようなセキュリティ対策を使っていればいいだろうということである。ただ，資料15に示したように，暗号技術の世界では，2010年問題というものが存在する。今使っている国際標準暗号方式は，米国政府が2010年までしか有効性の「お墨付き」を出していないという問題である。その先の技術も現在開発はされているのだが，いずれにしても，先を読んで対応していかなければいけないのが，暗号化技術の難しいところであり，そういう中で，金融機関は努力しているのである。

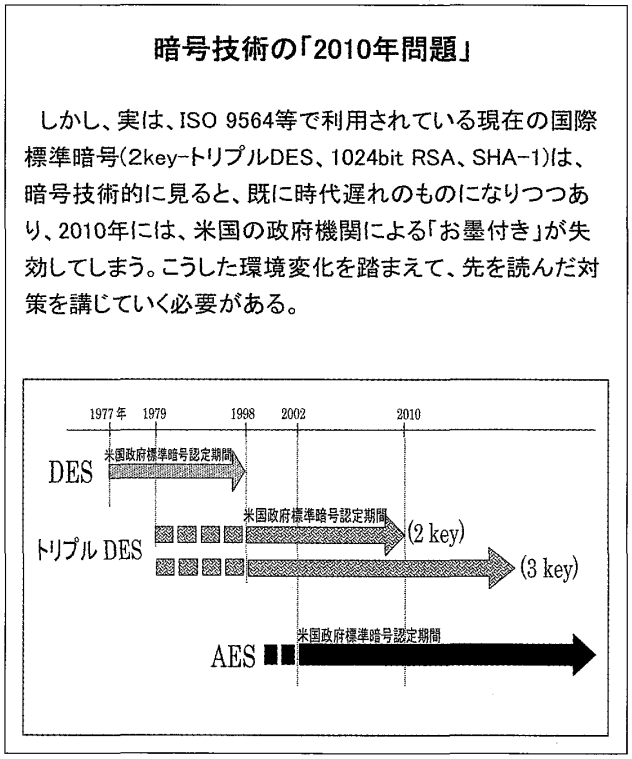
以上が，セキュリティ侵害に関する問題だが，金融界が，他の業種に比べて，セキュリティを重視すべきだと考える背景について，若干説明する。その背景とは，万一，セキュリティ侵害が発生した場合の被害が，他の業種よりも大きくなる危険性が高いということである。つまり，金融機関が取り扱うのは，取引金額や預金・貸出金の残高，金利や為替レートなど，金銭的な価値に関する情報そのもので，電子的な方法で処理されているそれらの情報は，わずかな改ざんでも巨額の不正に直結するからである。その点，他の産業では，ビジネスの対象物が限定されており，情報システムに不正があったとしても，それだけでは大きな被害につながりにくいと思われる。

3．3　業務継続計画（BCP：Business Continuity Plan）

安全なシステムを実現するために，大きな課題として残っているのが，業務継続計画（BCP）である。これは，資料16にあるが，2001年9月の米国同時多発テロ（9.11）を契機にクローズアップされた課題である。それまでは，言ってみれば，どこかひとつの拠点が災害等によりダウンする可能性があるとしても，バックアップをどこかに設置しておけば大丈夫だと考えていたのである。し



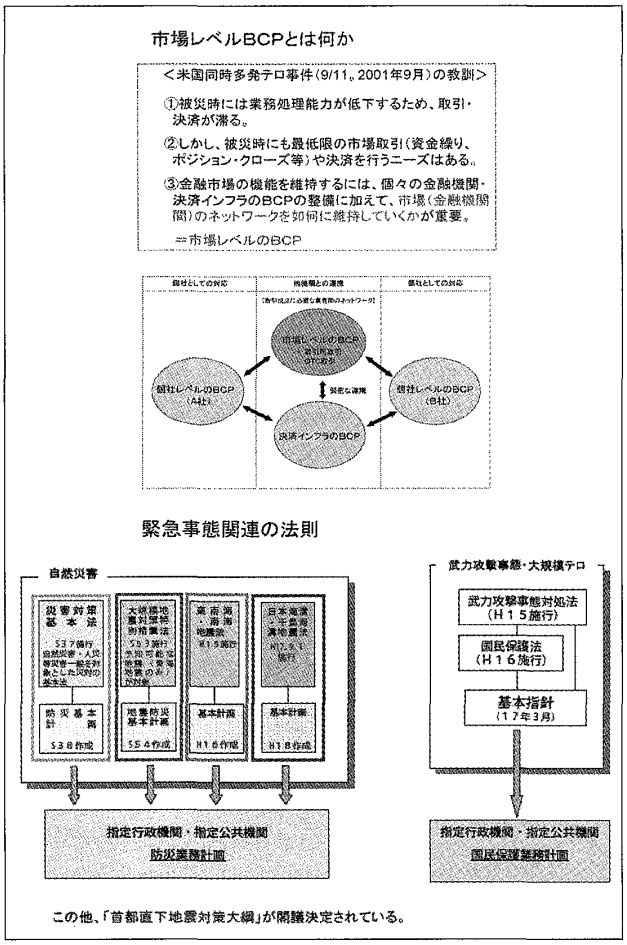
資料14



資料15

かし，同時に攻撃される可能性や，テロというのはこれだけ大きな被害を及ぼすということを改めて確認したのである。その時の米国では，国債の取引市場が２営業日間停止し，その後も１週間以上，正常な状態といえる状況ではなく，かなりの混乱が生じた。それを受けて，日本だけでなく世界各国が様々なBCP対応強化に取り組み始めたという流れである。金融市場全体の業務継続体制を強化していくには，個別の金融機関だけでなく，各種取引市場や決済インフラも相互に連携して体制整備を図っていくことが不可欠だ。現状は，資料16の右下のように，法律に基づき自然災害や武力攻撃等を想定した防災・国民保護の業務計画が着々とできており，それに沿った対応が進められている段階である。

ところで，大きな災害の事例としては，日本では阪神・淡路大震災というものが11年前に発生した。被災直後には，被災地域の金融機関の半分ぐらいの店舗が壊れて営業できない状態にあった。この時，日本銀行の神戸支店は，幸いにも壊れなかったため，建物の一部を，被災した金融機関の臨時窓口に提供するなどにより，現金の供給など金融機能の回復に努めた。非常時における金融の「最後の砦」の役割を果たしたということである。本日は，振替の話ばかり説明してきたが，一番プリミティブな決済手段は「現金」であり，現金を市中に供給することは日本銀行の重要な使命である。災害発生時には，命を守ることが最優先。次に電気，水道，ガスの確保が非常に重要であるが，経済活動を支える決済システムが基本機能を維持することも，同様に極めて重要である。決済ができない状況は，大変な混乱状態であるということを認識して欲しいと思う。なお，阪神・淡路大震災の際，日本銀行神戸支店は，被災当日から約40日間，土日無く金融機能の回復に奔走し，金融パニックを回避できたことに対して，危機管理の専門家等から高い評価をいただいたことを付け加えておきたい。



資料16

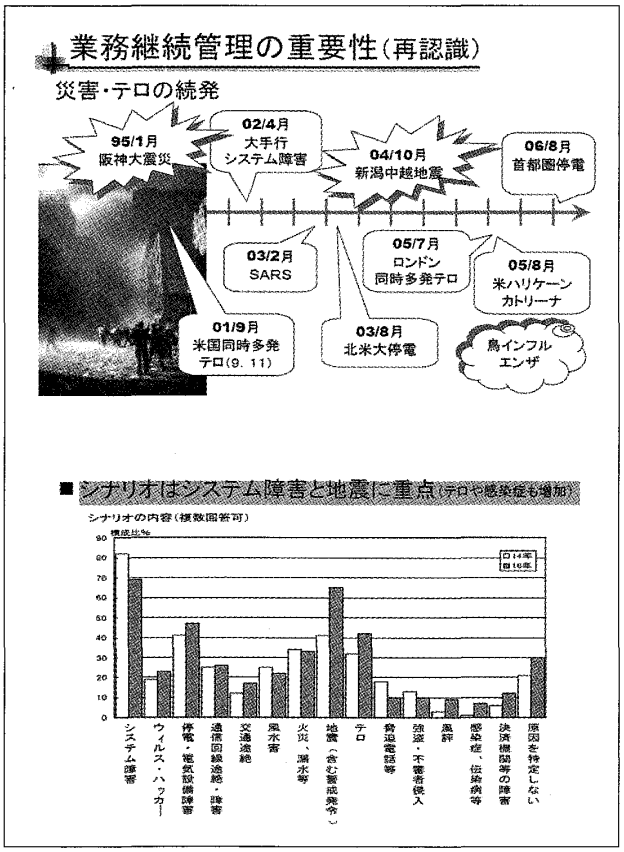
被災時の対応体制を整える時には，①バックアップシステムの持ち方，②要員の確保，③連絡網の整備，④決裁権限の明確化，⑤決裁権限者に支障がある時の対応，等を仔細にあらかじめ定めておき，それに基づいた訓練を行う際には，⑥どのような災害を想定するか，⑦優先すべき業務は何か，等に関して，複数のシナリオを策定して実施することが必要である。

全部の対策やシナリオの訓練を網羅的に実施できればいいのだが，時間の制約もあり，全部はできていない。それらの充実に向けて，金融界全体が不断に取り組んでいるのが現状である。なお，資料17に，業務継続管理が重要となる事象をまとめている。業務継続の危険性を孕む事象というものは，地震のほか，テロ，台風，感染症の流行，大規模システム障害，大規模停電など，様々なものがあるということを認識しておく必要がある。

以上のように，わが国の決済システムの現状からみて，安全で効率的な決済システムを目指して

の課題は少なくない。

言ってみれば，金融界は巨大な「装置産業」である。コンピュータを管理・運用する装置産業になっている以上，そこで利用している技術についての責任を感じないといけない。責任を持つということは，そこで使っている技術を分析・研究して，脅威を未然に取り除いていくことであり，金融界が対応しなければいけないことだと思っている。ただ，だからと言って，預金者はルーズでもいいのだということにはならないと私は思う。預金者保護法というものが成立して，被害にあっても金融界が補償してくれるじゃないか，というような意識，私たちはモラル・ハザードと呼ぶが，そういうものが生じた場合は，その意識が，セキュリティ対策がうまく機能しない状況をもたらすと考えて欲しいと思う。よく言われるのが，セキュリティ対策は，足し算じゃなく掛け算だというものである。つまり，金融界が100％のセキュリティ対応をしたとしても，利用者が，セキュリティに対してあいまいな考え方でルーズな対応をすると，100×0＝0ということで，セキュリティ対策は効果を発揮しないということである。極端な言い方ではあるが，少なくとも被害を小さくするためには，金融界だけが頑張っても限界がある。やはり利用者に一定の管理意識をしっかり持ってもらう。そうすれば，さきほど申し上げたような「二要素認証」ががっちり組み合って，セキュリティ対策が効果を発揮できることにつながる，と期待している。



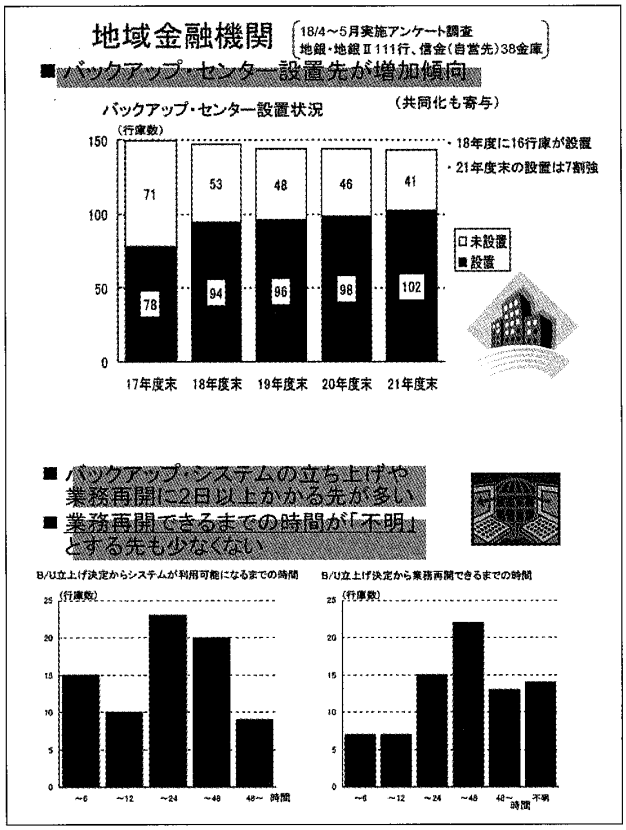
資料17

4．おわりに

本日の講演は，無用に不安心理をかき立ててしまう内容になったかも知れないが，それは私の本意ではない。現状について，正確には申し上げたが，不安を煽るような状況ではない。しかし，対策は真剣に考えて，より安全なシステムへの切り替えに，金融界は前向きに取り組んでいるということをお伝えしたかったわけである。そういう観点から，明るい話をふたつ述べておきたい。

まず，今年の６月頃に発表された大手監査法人の調査結果である。これは，世界の大手金融機関を対象としたセキュリティ調査で，これによると，地域別には日本の金融機関が過去１年間のセキュリティ対策において全地域中トップであったとの評価であった。日本の金融機関は，セキュリティ対応や個人情報の保護などの分野でとくに高い評価を受けている。

もうひとつは，先ほど説明した「BCP」に関して，全世界の金融監督機構が集まった会議（「ジョイント・フォーラム」）で，世界の被災等の実例を分析して，今後の改善策を提唱しようという動きである。多くのケース・スタディでは，要員確保や訓練ができていなかったとか，自家発電の施設が不十分であった等の反省が教訓として挙げられていた。そうした中で，日本の中越地震のケース・スタディでは，むしろ逆に，地域の金融機関の連絡体制の充実，その時の資金供給などの工夫，日頃の訓練の励行等が積極的な評価を受け，それを教訓として推奨するものであった。



資料18

このように，日本の金融機関は，不良債権問題で疲弊した体力を回復しつつある中で，安全で効率的な金融決済システムを目指して，前向きに取り組んでいるということを理解していただくとともに，皆さん各人が自分たちのできる範囲での「セキュリティ管理」をしっかりやってもらいたいということを，最後にお願いしておきたいと思う。

以　上

参考文献

1）青木周平，「決済の原理－決済についての入門講義－」，2001年
2）岩下直行，「偽造・盗難カード預貯金者保護法と金融機関のセキュリティ対策」，『ジュリスト』，2006年
3）――「金融機関の情報セキュリティ対策のあり方について」，『金融研究』第25巻別冊第１号，日本銀行金融研究所，2006年
4）――「金融高度化セミナー・金融業界における情報セキュリティ問題とその対策について」，2006年
5）遠藤勝裕，「阪神大震災－日銀神戸支店長の行動日記」，日本信用調査，1995年
6）金沢敏郎，「金融高度化セミナー・わが国における市場レベルBCPの現状と課題」，2006年
7）監査法人トーマツ，「2006 Global Security Survey」，2006年（http://tohmatsu.co.jp/news/2006/press0626.shtml）
8）ジョイント・フォーラム，「業務継続のための基本原則」，2006年
（http://www.boj.or.jp/type/release/zuiji_new/data/bis 0608a1.pdf）
9）富永新，「金融高度化セミナー・金融機関の業務継続強化に向けた課題と対応」，2006年
10）中山靖司，「インターネットバンキングの安全性を巡る現状と課題」，『日銀レビュー』，2006年
11）日本銀行，「決済システムレポート2005」，2006年
12）武藤敏郎，「決済システムと日本銀行」，2004年

（当解説は，平成18年10月25日開催の学術講演会における講演をもとに，改めて解説文として纏めたものである。）